AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Baiju V. Patel et al.	§	Group Art Unit:	2135
Serial No.:	09/364,835	§	Examiner:	Leynna A. Ha
Filed:	July 30, 1999	§	Assignee:	Intel Corporation
For:	Technique And Apparatus For Processing Cryptographic Services Of Data In A Network System	§	Atty. Dkt. No.:	ITL.0182US (P6867)

Mail Stop **Appeal Brief-Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Dear Sir:

Applicant's Reply to the Examiner's Answer is set forth below.

A. Are Claims 1-7, 16-20 and 28-37 Anticipated by U.S. Patent No. 5,546,463 (Caputo)?

Claim 1 specifies using a computer peripheral device to select a security service from other security service based on security information that is passed along with a data block. Applicant submits that the Examiner has failed to establish a *prima facie* case of anticipation for claim 1 for at least the following reasons.

In the Examiner's Answer, the Examiner contends that the language found in lines 1-12 in column 6 of Caputo discloses the security information of independent claim 1. Examiner's Answer, 13. Referring to the cited language, the cited language discloses "an

Date of Deposit: June 26, 2006
I hereby certify under 37 CFR 1.8(a) that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to Mail Stop **Appeal Brief-Patents**, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.
Janice Munoz
Janice Munoz

authentication number or digital signature, which is transmitted with data, for use in verifying its source and accuracy." Caputo, 6:11-12.

Given the Examiner's labeling of Caputo's authentication number or digital signature as the alleged security information of claim 1, a *prima facie* case of anticipation has not been set forth for claim 1 for at least the reason that Caputo fails to teach using a computer peripheral device to select a security service from other security services based on an authentication number or digital signature. More particularly, the Examiner refers to the language in lines 45-50 in column 5 of Caputo to allegedly teach the selection of a security service. Examiner's Answer, 14. However, the cited language merely refers to a number of purportedly well known encryption algorithms. This cited language does not, however, disclose a computer peripheral's selection of one of these encryption algorithms based on an authentication number or a digital signature. Quite to the contrary, Caputo states, "the choice of algorithm is unimportant to this invention." Caputo, 5:51-52. Caputo fails to teach the basis on which a particular algorithm is selected, fails to disclose the selection of an algorithm by a computer peripheral device, and thus, fails to teach or suggest that a computer peripheral selects a particular algorithm based on an authentication number or a digital signature.

Therefore, for at least the reason that the Examiner fails to show where Caputo allegedly teaches using a computer peripheral device to select a security service from other security services based on security information that is passed along with a data block, a *prima facie* case of anticipation has not been set forth for independent claim 1. As such, Applicant maintains that the § 102 rejection of claim 1 is in error and should be reversed.

A *prima facie* case of anticipation has also not been set forth for independent claim 16 for the reason that the Examiner fails to show where Caputo allegedly discloses a cryptographic engine that selects a security service from other security services based on security control information. The Examiner states, "the cryptographic engine is the modem," and refers to lines 18-22 in column 9 of Caputo to support this contention. Examiner's Answer, 15. However, neither the cited language nor any other portion of Caputo teaches or suggests a cryptographic engine that selects a security service from other security services based on security control information that is received by a receiving

circuit, as the rejections are based on the previously-discussed language found in lines 45-50 in column 5 of Caputo.

Thus, for at least these reasons, a *prima facie* case of anticipation has not been set forth for independent claim 16 and reversal of the rejection of this claim is requested.

Regarding the § 102 rejection of claim 28, claim 28 requires processing, in a computer peripheral device, a data block according to security information. The security information identifies at least one of an encryption algorithm and an authentication algorithm to be performed by the security service.

The Examiner refers to lines 1-12 of column 6, discussed above, to allegedly teach the security information of claim 28. Examiner's Answer, 15. The cited language merely discusses an authentication number or digital signature that verifies the source and accuracy of data. The cited language does not, however, disclose security information, which identifies one of an encryption algorithm and an authentication algorithm to be performed by a security service. More specifically, the language cited by the Examiner refers to *sender's* inclusion of an authentication number or digital signature in the data that is *transmitted* by the *sender* (*emphasis added*). A recipient of the data performs a verification process to determine if the data has been modified. Caputo, 6:15-18. However, Caputo fails to teach or suggest that the recipient selects a particular encryption or authentication algorithm based on the authentication number or digital signature. Without this disclosure, Caputo fails to anticipate independent claim 28.

Thus, Applicant maintains that the § 102 rejection of claim 28 in view of Caputo is in error and should be reversed.

Regarding independent claim 33, the Examiner refers to lines 18-22 of column 9 to allegedly disclose the cryptographic engine of claim 33. Examiner's Answer, 17. As discussed above, the purported cryptographic engine is the modem 40 of Caputo. Caputo fails to teach or suggest that the modem cryptographically processes data based on security control information, which identifies at least one of an encryption algorithm and an authentication algorithm to be performed on the data. Caputo fails to disclose that its authentication number or the digital signature identifies at least one an encryption algorithm and an authentication algorithm to be performed on data, and thus, a *prima facie*

case of anticipation has not been set forth for claim 33. As such, the § 102 rejection of claim 33 is in error and should be reversed.

B. Are Claims 13-15 Anticipated by U.S. Patent No. 5,268,962 (Abadi)?

The article of independent claim 13 recites instructions that when executed cause a system to determine from information in a data block if a security service has been performed on the data block by a computer peripheral device and process the data block if the security service has not been performed on the data block by the computer peripheral device.

In the Examiner's Answer, the Examiner appears to rely on Abadi's discussion of communications between host computers over a network. In particular, the Examiner appears to contend that Abadi's BQI value, which identifies a particular buffer queue in a receiving computer, constitutes the alleged information in a data block that identifies whether a security service has been performed on the data block by a computer peripheral device. *See, for example*, Examiner's Answer, 19. The Examiner cites language from lines 8-23 in column 6 of Abadi, language that states that upon a receiving host computer determining whether or not the BQI value is invalid or not, the host computer decides whether to discard or otherwise handle the data packet with an invalid BQI value.

However, the Examiner fails to establish a *prima facie* case of anticipation for independent claim 13 for at least the reason that the Examiner fails to show instructions that when executed cause a system to determine from information in a data block if a security service has been performed on the data block by *a computer peripheral device* (*emphasis added*). Thus, even assuming, for purposes of argument, that the BQI value somehow identifies whether or not a security service has been performed on a packet, Abadi fails to disclose information that identifies whether a security service has been performed on the packet by a computer peripheral device. Thus, claim 13 does not merely recite "a computer," but specifically sets forth "a computer peripheral device." The transmitting host computer, discussed in Abadi, is not a computer peripheral device. Thus, for at least this reason, a *prima facie* case of anticipation has not been set forth for independent claim 13.

Claims 14-15 are patentable for at least the reason that these claims depend from an allowable claim. Therefore, Applicant maintains that the § 102 rejections of claims 13-15 are in error and should be reversed.

The Commissioner is authorized to charge any fees or credit any overpayment to Deposit Account No. 20-1504 (ITL.0182US).

Respectfully submitted,

Date: June 26, 2006

Fred G. Pruner, Jr., Reg. No. 40,779
TROP, PRUNER & HU, P.C.
1616 S. Voss Road, Suite 750
Houston, TX 77057-2631
713/468-8880 [Phone]
713/468-8883 [Facsimile]

Attorneys for Intel Corporation

APPENDIX OF CLAIMS

The claims on appeal are:

1. A method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block;

generating security information to pass along with the data block, the security information identifying the security service;

using a computer peripheral device adapted to control communication with the communications channel to select the security service from other security services based on the security information; and

processing, in the computer peripheral device, the data block according to the security information.

2. The method of claim 1, wherein the processing includes performing cryptographic processing of the data block.

3. The method of claim 1, further comprising:

receiving the data block from a software routine; and

routing the processed data block back to the software routine after processing.

4. The method of claim 1, further comprising:

determining if the security service can be performed by the computer peripheral device; and

if not, processing the data block according to the security service in a software routine instead of the computer peripheral device.

5. The method of claim 1, further comprising identifying a security service according to an Internet Protocol security protocol.

13. An article including a machine-readable storage medium containing instructions for execution in a system including a computer peripheral device adapted to control communications with a communications channel, the instructions when executed causing the system to:

receive a data block from the computer peripheral device;

determine from information in the data block if a security service has been performed on the data block by the computer peripheral device; and

process the data block if the security service has not been performed on the data block by the computer peripheral device.

14. The article of claim 13, the storage medium containing instructions that when executed causes the system to retrieve security information associated with the data block and send the data block and security information to the computer peripheral device to perform the security service.

15. The article of claim 13, the storage medium containing instructions that when executed causes the system to perform the security service on the data block.

16. A controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data and associated security control information, the security control information identifying a security service to be performed on the data; and

a cryptographic engine to select the security service from other security services based on the security control information and cryptographically process the data based on the selection, the cryptographic engine being a computer peripheral device.

17. The controller of claim 16, further comprising a storage device containing information identifying security services to be performed, the received security control information selecting a portion of the security services information in the storage device, wherein the cryptographic engine processes the data according to the selected portion of the security services information.

18. The controller of claim 17, further comprising a device adapted to change the contents of the storage device to update the security services information.

19. The controller of claim 18, wherein the device is adapted to update the security services information based on a predetermined replacement policy.

20. The controller of claim 17, wherein the security services information includes security association information.

28. A method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block;

generating security information to pass along with the data block, the security information identifying at least one of an encryption algorithm and an authentication algorithm to be performed by the security service; and

processing, in a computer peripheral device adapted to control communication with the communications channel, the data block according to the security information.

29. The method of claim 28, wherein the processing includes performing cryptographic processing of the data block.

30. The method of claim 28, further comprising:

receiving the data block from a software routine; and

routing the processed data block back to the software routine after processing.

31. The method of claim 28, further comprising:

determining if the security service can be performed by the computer peripheral device; and

if not, processing the data block according to the security service in a software routine instead of the computer peripheral device.

32. The method of claim 28, further comprising identifying a security service according to an Internet Protocol security protocol.

33. A controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data and associated security control information, the security control information identifying at least one of an encryption algorithm and an authentication algorithm to be performed on the data; and

a cryptographic engine to cryptographically process the data based on the security control information, the cryptographic engine being a computer peripheral device.

34. The controller of claim 33, further comprising a storage device containing information identifying security services to be performed, the received security control information selecting a portion of the security services information in the storage device, wherein the cryptographic engine processes the data according to the selected portion of the security services information.

35. The controller of claim 34, further comprising a device adapted to change the contents of the storage device to update the security services information.

36. The controller of claim 35, wherein the device is adapted to update the security services information based on a predetermined replacement policy.

37. The controller of claim 34, wherein the security services information includes security association information.